

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 10271106 A

(43) Date of publication of application: 09.10.98

(51) Int. Cl. H04L 9/10
H04L 9/08

(21) Application number: 09068460

(22) Date of filing: 21.03.97

(71) Applicant: NIPPON TELEGR & TELEPH
CORP <NTT>

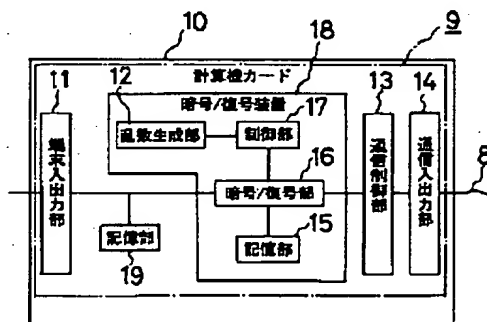
(72) Inventor: TAKADA SHUNSUKE
KAWAKUBO HIDEJI

(54) CIPHER COMMUNICATION METHOD AND
SYSTEM EQUIPMENT

(57) Abstract:

PROBLEM TO BE SOLVED: To perform the cipher communication of high safety by packaging and loading a secrecy protected ciphering/deciphering device to a computer card incorporated in a communication controller for connecting an information terminal equipment to a communication path and performing ciphering/ deciphering processings together for the transfer of the input/output of secret data between the information terminal equipment and the communication path.

SOLUTION: Through the terminal and communication input/output parts 11 and 14 and communication control part 13 of a cipher communication equipment 9 packaged to the computer card 10 and by the control, the information terminal equipments are connected by the communication path 8. A random number generation part 12 generates a random number and generates a cipher key, a storage part 15 stores the secret key and program of a transmission side for ciphering/deciphering and the storage part 19 stores the public key of a reception opposite side. A ciphering/deciphering part 16 executes the processing of ciphering/deciphering by using the cipher key and the public key by the control of a control part 17 and the ciphering/deciphering device 18 physically protects the secrecy of the respective parts inside. Thus, without uselessly consuming hardware resources, safe communication is made possible.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-271106

(43) 公開日 平成10年(1998)10月9日

(51) Int.Cl.⁸

H 0 4 L 9/10
9/08

識別記号

F I

H 0 4 L 9/00

6 2 1 A
6 0 1 A

審査請求 未請求 請求項の数19 O L (全 8 頁)

(21) 出願番号 特願平9-68460

(22) 出願日 平成9年(1997)3月21日

(71) 出願人 000004226

日本電信電話株式会社
東京都新宿区西新宿三丁目19番2号

(72) 発明者 高田 俊介

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(72) 発明者 河久保 秀二

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

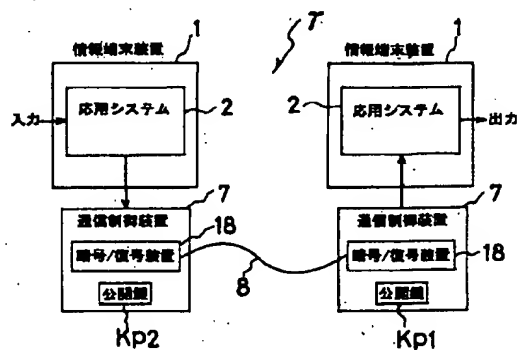
(74) 代理人 弁理士 菅 隆彦

(54) 【発明の名称】 暗号通信方法及びシステム装置

(57) 【要約】

【課題】 安全性が高く情報端末装置のハードウェアリソースを有効に利用出来る暗号通信方法及びシステム装置の提供。

【解決手段】 情報端末装置1を通信路8に接続する通信制御装置7に内蔵され、乱数生成部12と記憶部15と暗号/復号部16と制御部17とを備える暗号/復号装置18を搭載した暗号通信システム装置γの特徴。



【特許請求の範囲】

【請求項1】送信側で、

情報端末手段から受信したデータを機密が保護された手段内で生成した暗号鍵で暗号化した後、

公開鍵暗号方式の受信側の公開鍵で当該暗号鍵を暗号化した保護暗号鍵と先に暗号化された前記データを通信路に送信し、

受信側で、

当該通信路から受信した暗号化された前記保護暗号鍵を前記公開鍵と対応付けた受信側の秘密鍵で復号して送信側の前記暗号鍵を抽出した後、

当該暗号鍵で受信した前記暗号化データを復号する、
ことを特徴とする暗号通信方法。

【請求項2】機密保護手段は、

情報端末手段を通信路に接続する通信制御手段に内設する、

ことを特徴とする請求項1に記載の暗号通信方法。

【請求項3】機密保護手段は、

計算機カード内に実装搭載する、

ことを特徴とする請求項1又は2に記載の暗号通信方法。

【請求項4】通信路は、

電話回線、ISDN、LAN、無線、光通信、衛星通信等のいずれか又はこれ等の組合せである、

ことを特徴とする請求項1、2又は3に記載の暗号通信方法。

【請求項5】送受信両側は、

当該両側で通信制御手段の計算機カード内に自己の公開鍵とこれに対応付けた秘密鍵を格納するステップ1と、

送受信側を接続するステップ2と、

送信者の公開鍵情報を受信側に送信して受信側で送信者の公開鍵情報を蓄積するステップ3と、

受信者の公開鍵情報を送信側に送信して送信側で受信者の公開鍵情報を蓄積するステップ4と、

の前処理段階を順次踏む、

ことを特徴とする請求項1又は4に記載の暗号通信方法。

【請求項6】通信路への送信は、

パケット通信である、

ことを特徴とする請求項1、2、3、4又は5に記載の暗号通信方法。

【請求項7】保護暗号鍵は、

パケットのヘッダに添付して送信する、

ことを特徴とする請求項1、2、3、4、5又は6に記載の暗号通信方法。

【請求項8】送信側は、

暗号化したデータと保護暗号鍵をパケット通信後、

受信側の復号処理の出力完了まで送信及び受信を一時待機し、

受信側と相互交信のないことを確認した上で送信終了す

る、

後処理段階を順次踏む、

ことを特徴とする請求項1、2、3、4、5、6又は7に記載の暗号通信方法。

【請求項9】受信側は、

復号したデータを端末に出力した後、

送信側からの追加受信の余裕時間まで送信及び受信を一時待機し、

送信側と相互交信のないことを確認した上で通信終了する、

後処理段階を順次踏む、

ことを特徴とする請求項1、2、3、4、5、6、7又は8に記載の暗号通信方法。

【請求項10】通信路は、

インターネット、イントラネット、エキストラネット、OCN、ODN、仮想専用網、各種交換機網、VAN等に接続又は利用した暗号データ伝送路を形成する、

ことを特徴とする請求項1、2、3、4、5、6、7、8又は9に記載の暗号通信方法。

【請求項11】情報端末装置を通信路に接続する通信制御装置に内蔵され、

暗号／復号装置を搭載した、

ことを特徴とする暗号通信システム装置。

【請求項12】暗号／復号装置は、

機密を保護された装置である、

ことを特徴とする請求項11に記載の暗号通信システム装置。

【請求項13】暗号／復号装置は、

情報端末装置との入出力を制御する端末入出力部と、

受信相手側の公開鍵情報を格納する記憶部と、

通信路との入出力を制御する通信制御部と、

実際に通信路との入出力を行う通信入出力部と、共に、前記情報端末装置を前記通信路に接続する通信制御装置に内蔵する計算機カード上に一体に実装搭載する、

ことを特徴とする請求項11又は12に記載の暗号通信システム装置。

【請求項14】暗号／復号装置は、

暗号鍵を作成するための乱数を生成する乱数生成部と、

復号のための自己の秘密鍵やプログラムを蓄積する記憶部と、

前記暗号鍵を使用してデータの暗号／復号を行う暗号／復号部と、

暗号／復号の処理を制御する制御部と、を備える、

ことを特徴とする請求項11、12又は13に記載の暗号通信システム装置。

【請求項15】通信路は、

電話回線、ISDN、LAN、無線、光通信、衛星通信等のいずれか又はこれ等の組合せである、

ことを特徴とする請求項11、12、13又は14に記載の暗号通信システム装置。

【請求項16】通信路は、インターネット、イントラネット、エキストラネット、OCN、ODN、仮想専用網、各種交換機網、VAN等に接続又は利用した暗号データ伝送路を形成する、ことを特徴とする請求項11、12、13、14又は15に記載の暗号通信システム装置。

【請求項17】情報端末装置は、パソコン、ワークステーション、インテリジェント端末、電話器、FAX、交換機、電子メール端末、無線機、移動通信端末等を含む、ことを特徴とする請求項11、12、13、14、15又は16に記載の暗号通信システム装置。

【請求項18】受信相手側の公開鍵情報を格納する記憶部は、暗号／復号装置内の復号のための自己の秘密鍵やプログラムを蓄積する記憶部と兼用する、ことを特徴とする請求項13、14、15、16又は17に記載の暗号通信システム装置。

【請求項19】受信相手側の公開鍵情報を格納する記憶部は、暗号／復号装置内に復号のための自己の秘密鍵やプログラムを蓄積する記憶部と別に並設する、ことを特徴とする請求項13、14、15、16又は17に記載の暗号通信システム装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報端末装置を通して各種暗号データを相互交信するのに供される暗号通信方法及びその実施に直接使用するシステム装置に関する。

【0002】

【従来の技術】近年、オープンなネットワーク及びイントラネット等におけるリモートアクセスにおいて、情報の盗聴、改ざん、なりすましの脅威に対処する方法が検討されている。

【0003】従来、ネットワークで通信される情報を保護する方法において、図5に示すように情報端末装置1内の応用システム2に暗号／復号装置3と暗号鍵4を保持するシステム装置αや、図6に示すように計算機カードなどの外部記憶装置5内に暗号鍵6を保持するシステム装置βが知られている。なお、図中、7は通信制御装置、8は通信路である。

【0004】

【発明が解決しようとする課題】前述した従来の暗号方法において、図5の方法は秘密情報である暗号鍵4を情報端末装置1内に保持しその暗号鍵4を使用してメッセージを暗号化するシステム装置αを用いた手法である。この場合、通常暗号鍵4は秘密鍵などで暗号化して格納するが、実際に暗号処理を行う際に使用する暗号鍵4が復号されてメインメモリ上に展開されるため、盗聴され

る危険があり、また暗号鍵4の盗難や消去される危険がある。

【0005】図6の方法では、暗号鍵6を外部記憶装置5に保持し、情報端末装置1で暗号／復号処理を行う際に暗号鍵6を読み出して処理するシステム装置βを用いた手法である。この場合、暗号鍵6の盗難や消去に対する安全性は向上するが、処理実行中に暗号鍵6がメインメモリ上に展開される問題が解決できない。また、外部記憶装置5と通信制御装置7を同時に使用するため、情報端末装置1のハードウェアリソースの競合の問題も生ずる。

【0006】ここにおいて、本発明の解決すべき主要な目的は、次の通りである。本発明の第1の目的は、上記の問題を解決し、安全性が高く情報端末装置のハードウェアリソースを有効に利用できる暗号通信方法及びシステム装置を提供せんとするものである。

【0007】本発明の第2の目的は、通信制御装置内に暗号／復号装置を組み込んで暗号／復号処理を行う暗号通信方法及びシステム装置を提供せんとするものである。

【0008】本発明の第3の目的は、暗号鍵と秘密鍵と保護暗号鍵の三重鍵を駆使した暗号通信方法及びシステム装置を提供せんとするものである。

【0009】本発明の第4の目的は、暗号／復号装置を通信制御装置内に装備した計算機カードに秘密が保護されて実装搭載する暗号通信方法及びシステム装置を提供せんとするものである。

【0010】本発明のその他の目的は、明細書及び図面、特に特許請求の範囲の各請求項の記載から自ずと明らかとなる。

【0011】

【課題を解決するための手段】本発明は、前記課題を解決するのに当り、情報端末装置を通信路に接続する通信制御装置に内蔵した計算機カードに秘密が保護された暗号／復号装置を実装搭載し、前記情報端末装置と前記通信路間の秘密データの入出力のやり取りに際し、暗号／復号処理を併せ行う。

【0012】その際、前記暗号／復号装置内で作成した暗号鍵でデータを暗号化するとともに当該暗号鍵を公開鍵暗号方式の受信側の公開鍵で暗号化した保護暗号鍵を前記暗号化データと一緒に受信側に送信する。受信側では当該保護暗号鍵から前記公開鍵と対応付けた受信側の秘密鍵で暗号鍵を抽出し、その暗号鍵で暗号化データを復号処理する、所謂三重鍵をキーワードとして暗号解読のセキュリティを万全なものとしてある。特に電子マネーの授受に最適である。

【0013】さらに、具体的詳細に述べると、当該課題の解決では、本発明が次に列挙するそれぞれの新規な特徴的構成手法又は手段を採用することにより前記目的を達成する。

【0014】即ち、本発明方法の第1の特徴は、送信側で、情報端末手段から受信したデータを機密が保護された手段内で生成した暗号鍵で暗号化した後、公開鍵暗号方式の受信側の公開鍵で当該暗号鍵を暗号化した保護暗号鍵と先に暗号化された前記データを通信路に送信し、受信側で、当該通信路から受信した暗号化された前記保護暗号鍵を前記公開鍵と対応付けた受信側の秘密鍵で復号して送信側の前記暗号鍵を抽出した後、当該暗号鍵で受信した前記暗号化データを復号してなる暗号通信方法の構成採用にある。

【0015】本発明方法の第2の特徴は、前記本発明方法の第1の特徴における機密保護手段が、情報端末手段を通信路に接続する通信制御手段に内設してなる暗号通信方法の構成採用にある。

【0016】本発明方法の第3の特徴は、前記本発明方法の第1又は第2の特徴における機密保護手段が、計算機カード内に実装搭載してなる暗号通信方法の構成採用にある。

【0017】本発明方法の第4の特徴は、前記本発明方法の第1、第2又は第3の特徴における通信路が、電話回線、ISDN、LAN、無線、光通信、衛星通信等のいずれか又はこれ等の組合せである暗号通信方法の構成採用にある。

【0018】本発明方法の第5の特徴は、前記本発明方法の第1又は第4の特徴における送受信両側が、当該両側で通信制御手段の計算機カード内に自己の公開鍵とこれに対応付けた秘密鍵を格納するステップ1と、送受信側を接続するステップ2と、送信者の公開鍵情報を受信側に送信して受信側で送信者の公開鍵情報を蓄積するステップ3と、受信者の公開鍵情報を送信側に送信して送信側で受信者の公開鍵情報を蓄積するステップ4と、の前処理段階を順次踏んでなる暗号通信方法の構成採用にある。

【0019】本発明方法の第6の特徴は、前記本発明方法の第1、第2、第3、第4又は第5の特徴における通信路への送信が、パケット通信である暗号通信方法の構成採用にある。

【0020】本発明方法の第7の特徴は、前記本発明方法の第1、第2、第3、第4、第5又は第6の特徴における保護暗号鍵が、パケットのヘッダに添付して送信してなる暗号通信方法の構成採用にある。

【0021】本発明方法の第8の特徴は、前記本発明方法の第1、第2、第3、第4、第5、第6又は第7の特徴における送信側が、暗号化したデータと保護暗号鍵をパケット通信後、受信側の復号処理の出力完了まで送信及び受信を一時待機し、受信側と相互交信のないことを確認した上で送信終了する、後処理段階を順次踏んでなる暗号通信方法の構成採用にある。

【0022】本発明方法の第9の特徴は、前記本発明方法の第1、第2、第3、第4、第5、第6、第7又は第

8の特徴における受信側が、復号したデータを端末に出力した後、送信側からの追加受信の余裕時間まで送信及び受信を一時待機し、送信側と相互交信のないことを確認した上で通信終了する、後処理段階を順次踏んでなる暗号通信方法の構成採用にある。

【0023】本発明方法の第10の特徴は、前記本発明方法の第1、第2、第3、第4、第5、第6、第7、第8又は第9の特徴における通信路が、インターネット、イントラネット、エキストラネット、OCN、ODN、仮想専用網、各種交換機網、VAN等に接続又は利用した暗号データ伝送路を形成してなる暗号通信方法の構成採用にある。

【0024】本発明装置の第1の特徴は、情報端末装置を通信路に接続する通信制御装置に内蔵され、暗号／復号装置を搭載した暗号通信システム装置の構成採用にある。

【0025】本発明装置の第2の特徴は、前記発明装置の第1の特徴における暗号／復号装置が、機密を保護された装置である暗号通信システム装置の構成採用にある。

【0026】本発明装置の第3の特徴は、前記本発明装置の第1又は第2の特徴における暗号／復号装置が、情報端末装置との入出力を制御する端末入出力部と、受信相手側の公開鍵情報を格納する記憶部と、通信路との入出力を制御する通信制御部と、実際に通信路との入出力を行う通信入出力部と、共に、前記情報端末装置を前記通信路に接続する通信制御装置に内蔵する計算機カード上に一体に実装搭載してなる暗号通信システム装置の構成採用にある。

【0027】本発明装置の第4の特徴は、前記発明装置の第1、第2又は第3の特徴における暗号／復号装置が、暗号鍵を作成するための乱数を生成する乱数生成部と、復号のための自己の秘密鍵やプログラムを蓄積する記憶部と、前記暗号鍵を使用してデータの暗号／復号を行う暗号／復号部と、暗号／復号の処理を制御する制御部と、を備えてなる暗号通信システム装置の構成採用にある。

【0028】本発明装置の第5の特徴は、前記本発明装置の第1、第2、第3又は第4の特徴における通信路が、電話回線、ISDN、LAN、無線、光通信、衛星通信等のいずれか又はこれ等の組合せである暗号通信システム装置の構成採用にある。

【0029】本発明装置の第6の特徴は、前記本発明装置の第1、第2、第3、第4又は第5の特徴における通信路が、インターネット、イントラネット、エキストラネット、OCN、ODN、仮想専用網、各種交換機網、VAN等に接続又は利用した暗号データ伝送路を形成してなる暗号通信システム装置の構成採用にある。

【0030】本発明装置の第7の特徴は、前記本発明装置の第1、第2、第3、第4、第5又は第6の特徴にお

10

20

30

40

50

ける情報端末装置が、パソコン、ワークステーション、インテリジェント端末、電話器、FAX、交換機、電子メール端末、無線機、移動通信端末等を含んでなる暗号通信システム装置の構成採用にある。

【0031】本発明装置の第8の特徴は、前記本発明装置の第3、第4、第5、第6又は第7の特徴における受信相手側の公開鍵情報を格納する記憶部が、暗号/復号装置内の復号のための自己の秘密鍵やプログラムを蓄積する記憶部と兼用してなる暗号通信システム装置の構成採用にある。

【0032】本発明装置の第9の特徴は、前記本発明装置の第3、第4、第5、第6又は第7の特徴における受信相手側の公開鍵情報を格納する記憶部が、暗号/復号装置内に復号のための自己の秘密鍵やプログラムを蓄積する記憶部と別に並設してなる暗号通信システム装置の構成採用にある。

【0033】

【発明の実施の形態】本発明の実施の形態をその装置例及び方法例につき図面を参照して説明する。なお、本実施形態では、情報端末手段である情報端末装置はパソコン、ワークステーション、インテリジェント端末、電話器、FAX、交換機、電子メール端末、無線機、移動通信端末等を含み、通信路には電話回線、ISDN、LAN、無線、光通信、衛星通信等のいずれか又はこれ等の組合せで構成され、インターネット、イントラネット、エキストラネット、OCN、ODN、仮想専用網、各種交換機網、VAN等に接続又は利用した暗号データ伝送路を形成する。

【0034】(装置例) 図1は本装置例を組み込んだ暗号通信システム装置の構成ブロック図、図2は本装置例の構成ブロック図である。なお、図5乃至図6に示す従来例の暗号通信システム装置 α 、 β と同一装置及び部は同一符号を付して説明の重複を避けた。

【0035】図中、 γ は本装置例を装備した暗号通信システム装置、9は本装置例の暗号通信装置、10は暗号通信装置9を実装搭載する計算機カードの本体、11は情報端末装置1と計算機カード10の暗号通信装置9との入出力を制御する端末入出力部、12は暗号鍵 Ke_1 又は Ke_2 を作成するための乱数を生成する乱数生成部、13は通信路8との入出力を制御する通信制御部、14は実際に通信路8との入出力を行う通信入出力部である。

【0036】15は暗号/復号のための送信自己側の秘密鍵やプログラムを蓄積する記憶部、16は前記暗号鍵 Ke_1 又は Ke_2 や前記公開鍵 Kp_1 又は Kp_2 や秘密鍵(図示せず)を使用して実際に暗号/復号を行う暗号/復号部、17は暗号/復号の処理を制御する制御部、18は乱数生成部12と記憶部15と暗号/復号部16と制御部17の機密を物理的に保護する暗号/復号装置、19は受信相手側の公開鍵 Kp_2 情報などを格納す

る記憶部である。なお、記憶部19を記憶部15と兼用しても良いし、記憶部19を暗号/復号装置18内に記憶部15と並存しても一向に構わない。

【0037】(方法例) 当該本装置例に適用する本方法例の実行手順を図面について説明する。図3は本方法例の暗号通信処理手順を示すフローチャート、図4は同・シーケンスチャートである。

【0038】(1) 通信前処理段階X

まず、本方法例で使用する計算機カード10発行時にそのカード10の秘密情報である公開鍵暗号方式の自己の公開鍵 Kp_1 (Kp_2)に対応付けた図示しない秘密鍵を記憶部15に、公開鍵 Kp_1 (Kp_2)を記憶部19にそれぞれ格納し(ST1)、相手側の公開鍵 Kp_2 (Kp_1)を記憶部19に格納する。

【0039】利用者Aと利用者Bは、電話回線、ISDN、LAN、無線、光通信、衛星通信等においてそれぞれ通常行われる接続要求情報S1と接続許可情報S2との交信手順により相互接続を確立(ST2)、利用者Aが使用する計算機カード10の公開鍵情報 Kp_1 と利用者Bが使用する計算機カード10の公開鍵情報 Kp_2 をそれぞれ交換して蓄積する(ST3, ST4)。

【0040】(2) 暗号/復号交信処理段階Y

利用者Aの送信側では、送信処理は、情報端末装置1からの送信データM1を端末入出力部11で受信し(ST5)、送信データM1と受信側の公開鍵 Kp_2 を物理的に機密が保護された暗号/復号装置18に送る。暗号/復号装置18では、まず制御部17が乱数生成部12で生成した乱数により暗号鍵 Ke_1 を生成する(ST6)。

【0041】次に、記憶部15に格納されている暗号プログラムを呼び出し、暗号鍵 Ke_1 を使用して暗号/復号部16で送信データM1を暗号化する(ST7)。さらに制御部17は記憶部15に格納されている公開鍵暗号プログラムを呼び出し、受信側の公開鍵 Kp_2 を使用して暗号/復号部16で暗号鍵 Ke_1 を暗号化する(ST8)。その上、通信制御部13は、暗号化した送信データ $Ke_1[M1]$ にヘッダ情報として暗号化した保護暗号鍵 $Kp_2[Ke_1]$ を付加したデータ $Ke_1[M1]$ を受取り、通信入出力部14から通信路8に送出する(ST10)。

【0042】他方、利用者Bの受信側では、受信側の計算機カード10上の通信制御部13が通信入出力部14で通信路8からのデータ $Kp_2[Ke_1] \cdot Ke_1[M1]$ を受信し(ST6')、暗号/復号装置18に送る。暗号/復号装置18では、制御部17が受信データ $Kp_2[Ke_1] \cdot Ke_1[M1]$ から保護暗号鍵 $Kp_2[Ke_1]$ を抽出して(ST7')、記憶部15に格納されている公開鍵暗号プログラムと自分の公開鍵 Kp_2 に対応付けた図示しない秘密鍵を呼び出し、自分の秘密鍵で保護暗号鍵 $Kp_2[Ke_1]$ を暗号鍵 Ke_1 に復

号する(ST8')。

【0043】さらに制御部17は、記憶部15から復号プログラムを呼び出し暗号鍵Ke1で暗号化された送信データKe1[M1]を復号し受信データM1を抽出する(ST9')。最後に抽出した受信データM1を端末入出力部11から情報端末装置1に出力する(ST10')。

【0044】(3) 後処理段階Z

利用者Aの送信側では、受信側の通信制御装置7で最終復号処理した受信データM1を情報端末装置1に出力完了するまで送信及び受信を一時待機し(ST11)、その後受信側と相互交信のないことを確認した上で通信終了する(ST12)。又、利用者Bの受信側では、送信側からの追加受信の余裕時間まで送信及び受信を一時待機し(ST11')、送信側と相互交信のないことを確認した上で通信終了する(ST12')。

【0045】

【発明の効果】以上述べたように本発明によれば、計算機カード内に電話回線、ISDN、LAN、無線、光通信などの通信装置と暗号/復号装置を持ち、また鍵の生成から暗号/復号処理までを機密が保護された装置内でのみ行うことにより、通信プログラムなどの応用システムに影響をおよぼさず、ハードウェアリソースを浪費することなく、安全な通信を実現できる。

【図面の簡単な説明】

【図1】本発明の実施形態を示す装置例を組み込んだ暗号通信システム装置の構成ブロック図である。

【図2】同上装置例の構成ブロック図である。

【図3】本発明の実施の形態を示す方法例の暗号通信処理手順を示すフローチャートである。

【図4】同上方法例のシーケンスチャートである。

【図5】従来例の暗号通信システム装置の構成ブロック図である。

【図6】他の従来例の暗号通信システム装置の構成ブロック図である。

【符号の説明】

α, β, γ…暗号通信システム装置

1…情報端末装置

2…応用システム

3, 18…暗号/復号装置

4, 6…暗号鍵

5…外部記憶装置

7…通信制御装置

8…通信路

9…暗号通信装置

10…計算機カード

11…端末入出力部

12…乱数生成部

13…通信制御部

14…通信入出力部

15, 19…記憶部

16…暗号/復号部

17…制御部

18…暗号/復号装置

Kp1, Kp2…公開鍵

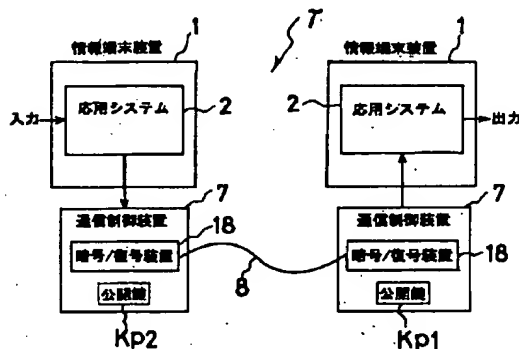
Ke1, Ke2…暗号鍵

M1, M2…送・受信データ

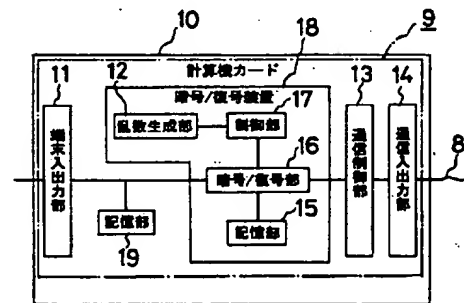
Ke1[M1], Ke2[M2]…暗号化データ

Kp1[Ke2], Kp2[Ke1]…保護暗号鍵

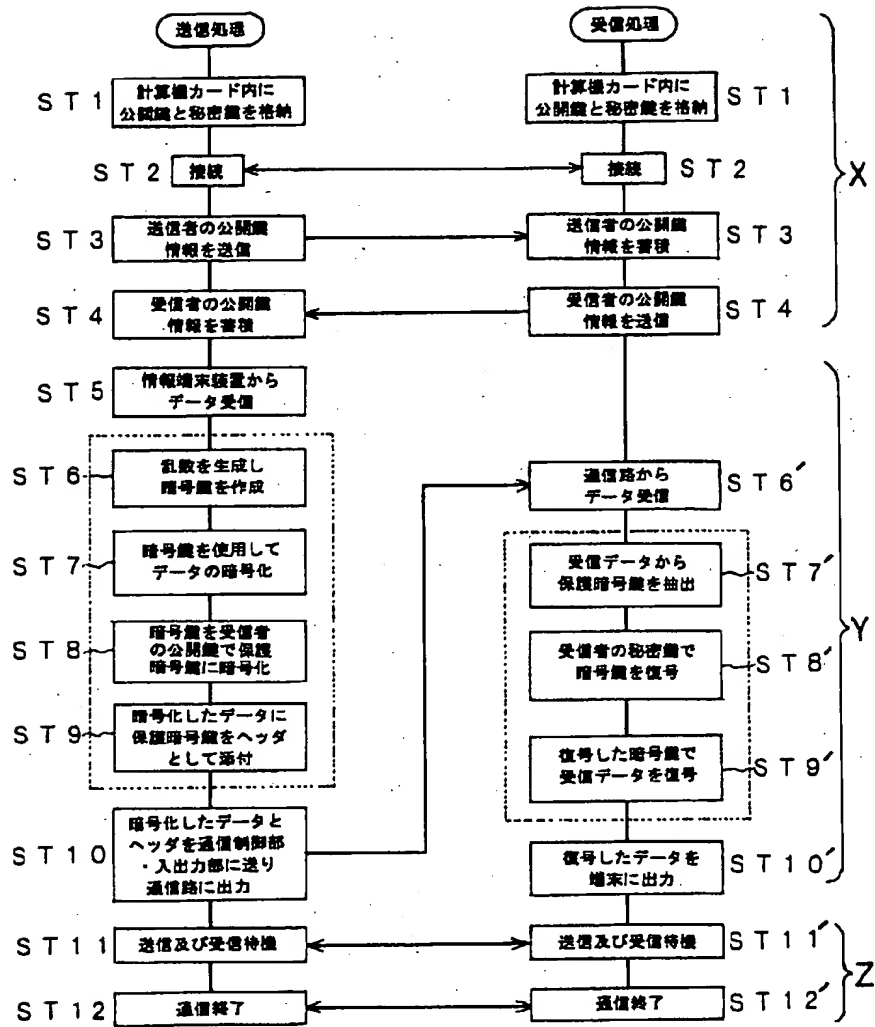
【図1】



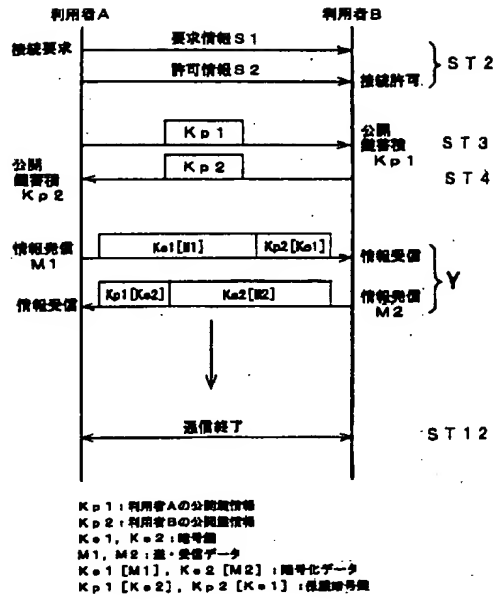
【図2】



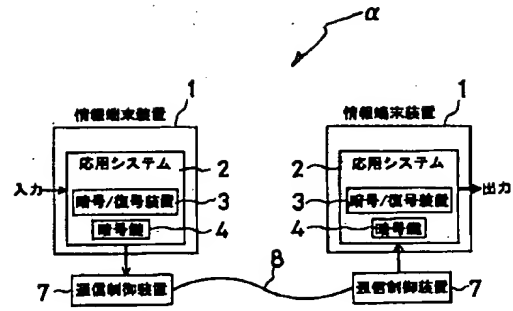
【図3】



【図4】



【図5】



【図6】

